ASYMPTOTICALLY GOOD 4-QUASI TRANSITIVE ALGEBRAIC GEOMETRY CODES OVER PRIME FIELDS

MARÍA CHARA, RICARDO TOLEDANO,
RICARDO PODESTÁ

Abstract. We study the asymptotic behavior of a family of algebraic geometry codes which are 4-quasi transitive linear codes. We prove that this family is asymptotically good over many prime fields using towers of algebraic function fields.

1. Introduction

It was proved in [12] and [2] that several classes of algebraic geometry codes, such as transitive codes, self-dual codes and quasi transitive codes among others, are asymptotically good over finite fields with square and cubic cardinality. Similar results were proved in [3] for general non-prime fields. In fact, some of them attain the well known Tsfasman-Vladut-Zink bound and also improvements for another well known bound of Gilbert-Varshamov were given. These results were achieved by considering algebraic geometry codes associated to asymptotically good towers of function fields over suitable finite fields.

Remarkably few things are known with respect to the behavior of families of AG-codes over prime fields with some additional structure, besides linearity. One reason for this situation is that the main tool used to produce good sequences of AG-codes is the Galois closure of some asymptotically good recursive tower of function fields and, so far, no recursive tower has been found to be asymptotically good over a prime field. The main goal of this work is to prove the existence of asymptotically good 4-quasi transitive codes over many prime fields.

An outline of the paper is as follows. In Section 2 we review the basic definitions and concepts on algebraic codes, algebraic-geometry codes (AG-codes for short) and the notion of their asymptotic behavior, which will be used throughout the paper. In Section 3, we review the standard way to get asymptotically good sequences of AG-codes attaining what we call a (λ, δ)-bound (see Definition 2.1).

In Section 4 we prove the main result, Theorem 4.1, asserting that the existence of a separable polynomial over $\mathbb{F}_q$ with certain properties implies that there are asymptotically good 4-quasi transitive codes over $\mathbb{F}_q$ in odd characteristic. In Corollary 4.2 we show how to obtain a concrete polynomial where these properties are computationally simple to check. In this way we can prove that there are asymptotically good 4-quasi transitive codes over $\mathbb{F}_p$ for infinitely many primes p having a concrete form such as, for instance, primes of the form $p = 220n + 1$ or $p = 232n + 1$. In fact, using Corollary 4.2, it is easy to check that there exist asymptotically good sequences of 4-quasi transitive linear codes over $\mathbb{F}_p$ for each prime $13 \leq p \leq M$ for large values of M, say $M = 10^6$. All of this suggests that the same conclusion must hold for any prime $p \geq 13$.

Key words and phrases. AG-codes, algebraic function fields, asymptotic goodness, towers.
2010 *Mathematics Subject Classification.* Primary 58J28; Secondary 58Cxx, 20H15, 11M35.
Partially supported by CONICET, UNL CAI+D 2011, SECyT-UNC, CSIC.

Finally, in Section 5, we consider a distinguished subclass of transitive codes, namely, the class of cyclic codes. The asymptotic behavior of this class is a a long standing open problem in coding theory. We prove that the methods used for the cases of transitive or quasi-transitive AG-codes, i.e. those ones using asymptotically good towers of function fields and automorphisms, are rather unsuited to deal with these problems.

2. Preliminaries

A linear code of length n, dimension k and minimum distance d over a finite field $\mathbb{F}_q$ with q elements, is simply an $\mathbb{F}_q$-linear subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ with $k = \dim \mathcal{C}$ and $d = \min\{d(c, c') : c, c' \in \mathcal{C}, c \neq c'\}$, where d is the Hamming distance in $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are usually called codewords and it is customary to say that $\mathcal{C}$ is an $[n, k, d]$-code over $\mathbb{F}_q$. By using the standard inner product in $\mathbb{F}_q^n$ we have the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ which is just the dual of $\mathcal{C}$ in $\mathbb{F}_q^n$ as a $\mathbb{F}_q$-vector space. A code $\mathcal{C}$ is called *self-dual* if $\mathcal{C}^\perp = \mathcal{C}$.

Transitive and quasi transitive codes. There is a natural action of the permutation group $\mathbb{S}_n$ on $\mathbb{F}_q^n$ given by

$$\pi \cdot (v_1, \dots, v_n) = (v_{\pi(1)}, \dots, v_{\pi(n)})$$

where $\pi \in \mathbb{S}_n$ and $(v_1, \dots, v_n) \in \mathbb{F}_q^n$. The set of all $\pi \in \mathbb{S}_n$ such that $\pi \cdot c \in \mathcal{C}$ for all codewords c of $\mathcal{C}$ forms a subgroup $\mathrm{Perm}(\mathcal{C})$ of $\mathbb{S}_n$ which is called the *permutation group* of $\mathcal{C}$ (sometimes denoted by $\mathrm{PAut}(\mathcal{C})$), that is

$$\mathrm{Perm}(\mathcal{C}) = \{\pi \in \mathbb{S}_n : \pi(\mathcal{C}) = \mathcal{C}\}.$$

A code $\mathcal{C}$ is called *transitive* if $\mathrm{Perm}(\mathcal{C})$ acts transitively on $\mathcal{C}$, i.e. for any $c \in \mathcal{C}$ and $1 \leq i < j \leq n$ there exists $\pi \in \mathrm{Perm}(\mathcal{C})$ such that $\pi(i) = j$. An important particular case of the class of transitive codes is the class of *cyclic* codes. These are the ones which are invariant under the action of the cyclic shift $s \in \mathbb{S}_n$ defined as $s(1) = n$ and $s(i) = i - 1$ for $i = 2, \dots, n$, i.e. a code $\mathcal{C}$ is cyclic if $s \cdot c \in \mathcal{C}$ for every $c \in \mathcal{C}$.

Suppose now that $n = rm$ for some positive integers r and m. We have an action of $\mathbb{S}_m$ on $\mathbb{F}_q^n$ as follows: we consider any $v \in \mathbb{F}_q^n$ divided into r consecutive blocks of m coordinates

$$v = (v_{1,1}, \dots, v_{1,m}, v_{2,1}, \dots, v_{2,m}, \dots, v_{r,1}, \dots, v_{r,m}),$$

and if $\pi \in \mathbb{S}_m$ we define the action block by block, i.e.

$$\pi \cdot v = (v_{1,\pi(1)}, \dots, v_{1,\pi(m)}, v_{2,\pi(1)}, \dots, v_{2,\pi(m)}, \dots, v_{r,\pi(1)}, \dots, v_{r,\pi(m)}).$$

The set of all $\pi \in \mathbb{S}_m$ such that $\pi \cdot c \in \mathcal{C}$ for all words c of $\mathcal{C}$ forms a subgroup $\mathrm{Perm}_r(\mathcal{C})$ of $\mathbb{S}_m$ which is called the r-permutation group of $\mathcal{C}$. A code $\mathcal{C}$ is called *r-quasi transitive* if $\mathrm{Perm}_r(\mathcal{C})$ acts transitively on each of the r blocks of every word of $\mathcal{C}$, i.e. for any $c \in \mathcal{C}$ and $1 \leq i < j \leq m$ there exists $\pi \in \mathrm{Perm}_r(\mathcal{C})$ such that $\pi(i) = j$. Note that 1-quasi transitive codes are just the transitive codes.

Asymptotic behavior. It is convenient to normalize the dimension and minimum distance of a code $\mathcal{C}$ with respect to the length n so that the *information rate* $R = R(\mathcal{C}) := k/n$ and the *relative minimum distance* $\delta = \delta(\mathcal{C}) := d/n$ of $\mathcal{C}$ are in the unit interval for any $[n, k, d]$-code $\mathcal{C}$. The goodness of a $[n, k, d]$-code over $\mathbb{F}_q$ is usually measured according to how big the sum $R + \delta = k/n + d/n$ is. Since k and d can not be arbitrarily large for n fixed, it is natural to allow arbitrarily large lengths, i.e. it is natural to consider a sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ such that $n_i \to \infty$ as $i \to \infty$ and see how big the sum $k_i/n_i + d_i/n_i$ can be as $n_i \to \infty$.

A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ is called *asymptotically good over* $\mathbb{F}_q$ if

$$\limsup_{i\to\infty} \frac{k_i}{n_i} > 0 \qquad \text{and} \qquad \limsup_{i\to\infty} \frac{d_i}{n_i} > 0$$

where $n_i \to \infty$ as $i \to \infty$.

Definition 2.1. Let $\lambda \in (0,1)$ and let $r = \lambda - \delta > 0$ where $\lambda > \delta > 0$. A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ is said to attain an (λ, δ)- *bound over* $\mathbb{F}_q$ if

$$\limsup_{i\to\infty} \frac{k_i}{n_i} \geq r \qquad \text{and} \qquad \limsup_{i\to\infty} \frac{d_i}{n_i} \geq \delta\,.$$

Thus a lower bound for the above mentioned goodness of a code is obtained for a sufficiently large index i since

$$\frac{k_i}{n_i} + \frac{d_i}{n_i} \sim r + \delta = \lambda,$$

as $i \to \infty$. In other words, we say more than the good asymptotic behavior of the sequence of codes $\{\mathcal{C}_i\}_{i=0}^{\infty}$.

Consider now the so called Ihara's function (see, for instance, [9] and [13])

$$A(q) \colon = \limsup_{g\to\infty} \frac{N_q(g)}{g}\,,$$

where $N_q(g)$ is the maximum number of rational places that a function field over $\mathbb{F}_q$ of genus g can have. It was proved by Serre ([10]) that $A(q) \geq c \log q$ for some positive constant c and by Drinfeld and Vladut ([15]) that $A(q) \leq \sqrt{q} - 1$. There are several improvements and refinements of lower bounds for $A(q)$ as can be seen in [9].

Let $\{\mathcal{C}_i\}_{i=0}^{\infty}$ be a sequence of codes over $\mathbb{F}_q$ such that $A(q) > 1$. The sequence is said to attain the *Tsfasman-Vladut-Zink bound over* $\mathbb{F}_q$ if it attains an (λ, δ)-bound with $\lambda = 1 - A(q)^{-1}$. This special (λ, δ)-bound gives a lower bound for the so called Manin's function $\alpha_q(\delta)$. More precisely

$$\alpha_q(\delta) \colon = \limsup_{n\to\infty} \tfrac{1}{n} \log_q A_q(n, \lfloor \delta n \rfloor) \geq 1 - \frac{1}{A(q)} - \delta,$$

where $0 \leq \delta \leq 1$ and $A_q(n,d)$ denotes the maximum number of words that a code over $\mathbb{F}_q$ of length n and minimum distance d can have. For squares $q \geq 49$, the Tsfasman-Vladut-Zink bound over $\mathbb{F}_q$ improves the Gilbert-Varshamov bound which was considered, for some time, the best lower bound for Manin's function (see [13], [12] and [14]).

AG-codes. Many families of linear codes over $\mathbb{F}_q$ have been proved to attain the above mentioned Tsfasman-Vladut-Zink bound using Goppa ideas for constructing linear codes from the set of rational points of algebraic curves over $\mathbb{F}_q$. These linear codes are called *algebraic geometry* codes (or simply AG-codes) and some standard references for AG-codes are the books [13], [14], [7], [8] and [11]. We recall now their construction using the terminology of function fields (instead of algebraic curves) following [13]. Let F be an algebraic function field over $\mathbb{F}_q$, let $D = P_1 + \cdots + P_n$ and G be divisors of F with disjoint supports, where $P_1, \ldots, P_n$ are different rational places of F. Consider now the Riemann-Roch space associated to G

$$\mathcal{L}(G) = \{u \in F \setminus \{0\} : (u) \geq -G\} \cup \{0\}, \tag{2.1}$$

where (u) denotes the principal divisor associated to $u \in F$. The AG-code defined by F, D and G is

$$\mathcal{C} = C_{\mathcal{L}}(D, G) = \big\{\big(u(P_1), u(P_2), \ldots, u(P_n)\big) \in \mathbb{F}_q^n : u \in \mathcal{L}(G)\big\}, \tag{2.2}$$

where $u(P_i)$ stands for the residue class of x modulo P_i.

An important feature of these codes is that lower bounds for their dimension k and minimum distance d are available in terms of the genus $g(F)$ of F and the degree $\deg G$ of G. More precisely,

(i) $k \geq \deg G + 1 - g(F)$ if $\deg G < n$, and

(ii) $d \geq n - \deg G$.

Furthermore, if $2g(F) - 2 < \deg G < n$ then $k = \deg G + 1 - g(F)$.

In view of the usefulness of AG-codes in asymptotic problems, the following question is of interest in the theory of AG-codes: *given a function field F over $\mathbb{F}_q$, how can we construct an AG-code with some prescribed property, besides linearity?* Something can be achieved in this direction by considering a finite and separable extension F of a rational function field $\mathbb{F}_q(x)$ and using the action of the group $\mathrm{Aut}(F/\mathbb{F}_q(x))$ of $\mathbb{F}_q(x)$-automorphisms of F on the places of F. It is well known (see, for instance, [13]) that $\mathrm{Aut}(F/\mathbb{F}_q(x))$ acts on the set of all places of F and this action is extended naturally to divisors. Even more, if $F/\mathbb{F}_q(x)$ is Galois extension and $\{P_1, \ldots, P_n\}$ is the set of of all places of F lying above a place P of $\mathbb{F}_q(x)$, then for each $1 \leq i < j \leq n$ there exists $\sigma \in \mathrm{Gal}(F/\mathbb{F}_q(x))$ such that $\sigma(P_i) = P_j$. This means that $\mathrm{Gal}(F/\mathbb{F}_q(x))$ acts transitively on the set $\{P_1, \ldots, P_n\}$.

Suppose now that $\sigma(G) = G$ for any $\sigma \in H$ where H is a subgroup of $\mathrm{Aut}(F/\mathbb{F}_q(x))$. Then there is an action of H on $C_{\mathcal{L}}(D, G)$ defined as

$$\sigma \cdot \big(u(P_1), u(P_2), \ldots, u(P_n)\big) := \big(u(\sigma(P_1)), u(\sigma(P_2)), \ldots, u(\sigma(P_n))\big).$$

It is clear that all of this implies that the AG-code $C_{\mathcal{L}}(D, G)$ is transitive if H acts transitively on the set $\{P_1, \ldots, P_n\}$. Similarly, if H is a cyclic group then, under the above conditions, the AG-code $C_{\mathcal{L}}(D, G)$ is cyclic (see Section 5 for a more detailed discussion). For self-duality, just a prime element t for all the places $P_1, \ldots, P_n$ is needed. Then if $2G - D$ is the principal divisor (dt/t), it can be proved that the AG-code $C_{\mathcal{L}}(D, G)$ is self-dual (see Chapter 8 of [13]).

3. Good AG-codes from sequences of function fields

Let K be a perfect field. A function field (of one variable) F over K is a finite algebraic extension F of the rational function field $K(x)$, where x is a transcendental element over K. Following [13], a *tower* $\mathcal{F}$ (of function fields) over a perfect field K is a sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over K such that

(1) $F_i \subsetneq F_{i+1}$ for all $i \geq 0$.

(2) The extension F_{i+1}/F_i is finite and separable, for all $i \geq 1$.

(3) The field K is algebraically closed in F_i, for all $i \geq 0$.

(4) The genus $g(F_i)$ of F_i tends to infinity, for $i \to \infty$.

A tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over K is called *recursive* if there exist a sequence of transcendental elements $\{x_i\}_{i=0}^{\infty}$ over K and a bivariate polynomial $H(X, Y) \in K[X, Y]$ such that $F_0 = K(x_0)$ and

$$F_{i+1} = F_i(x_{i+1}), \quad \text{where } H(x_i, x_{i+1}) = 0,$$

for all $i \geq 0$.

Now we define the concept of the asymptotic behavior of a tower over K. Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a tower of function fields over K. The *genus* $\gamma(\mathcal{F})$ of $\mathcal{F}$ over F_0 is defined as

$$\gamma(\mathcal{F}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}\,.$$

When K is a finite field, we denote by $N(F_i)$ the number of rational places (i.e., places of degree one) of F_i and the *splitting rate* $\nu(\mathcal{F})$ of $\mathcal{F}$ over F_0 is defined as

$$\nu(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}.$$

A tower $\mathcal{F}$ is called *asymptotically good* over a finite field K if

$$\nu(\mathcal{F}) > 0 \qquad \text{and} \qquad \gamma(\mathcal{F}) < \infty.$$

Otherwise is called *asymptotically bad*. Equivalently, a tower $\mathcal{F}$ is asymptotically good over a finite field K if and only if *the limit* of the tower $\mathcal{F}$

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)},$$

is positive, where $g(F_i)$ stands for the genus of F_i.

There is an standard way to construct a sequence of AG-codes over a finite field $\mathbb{F}_q$ attaining a (λ, δ)-bound as we show in the following lemma. We include the proof for the convenience of the reader.

Proposition 3.1. *Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a sequence of algebraic function fields over $\mathbb{F}_q$ with $\mathbb{F}_q$ as their full field of constants and such that for each $i \geq 1$ there are n_i rational places $P_1^{(i)}, \ldots, P_{n_i}^{(i)}$ in F_i with $n_i \in \mathbb{N}$. Let $\ell \in (0, 1)$ and suppose that the following conditions hold:*

(a) *$n_i \to \infty$ as $i \to \infty$,*

(b) *there exists an index i_0 such that $\frac{g(F_i)}{n_i} \leq \ell$ for all $i \geq i_0$, and*

(c) *for each $i > 0$ there exists a divisor G_i of F_i whose support is disjoint from the support of $D_i := P_1^{(i)} + \cdots + P_{n_i}^{(i)}$ such that*

$$\deg G_i \leq n_i\, s(i),$$

where $s : \mathbb{N} \to \mathbb{R}$ with $s(i) \to 0$ as $i \to \infty$.

Then there exists a sequence of positive integers $\{r_i\}_{i=m}^{\infty}$ such that $\mathcal{F}$ induces a sequence $\mathcal{G} = \{\mathcal{C}_i\}_{i=m}^{\infty}$ of asymptotically good AG-codes of the form $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$ attaining a (λ, δ)-bound with $\lambda = 1 - l$ and $0 < \delta < \lambda$.

Proof. Let $\delta \in (0, 1)$ be a fixed real number such that $1 - \delta > \ell$. Note that δ depends only on ℓ. For any given $\epsilon > 0$ such that $\epsilon < 1 - \delta$ there exists an index $i_\epsilon > 0$ such that

$$\frac{\deg G_i}{n_i} < \epsilon$$

for all $i \geq i_\epsilon$. Clearly, we can find a positive integer r_i such that

$$1 - \delta \geq r_i \frac{\deg G_i}{n_i} > 1 - \delta - \epsilon\,. \tag{3.1}$$

Let us consider now the AG-code $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$ for $i \geq i_0$. This is a code of length n_i and we have that its minimum distance d_i satisfies

$$d_i \geq n_i - r_i \deg G_i\,.$$

From this and the left hand side inequality in (3.1) we see that the relative minimum distance $\mathcal{C}_i$ satisfies

$$\frac{d_i}{n_i} \geq 1 - r_i \frac{\deg G_i}{n_i} \geq \delta.$$

On the other hand, for the dimension k_i of $\mathcal{C}_i$ we have

$$k_i \geq r_i \deg G_i + 1 - g(F_i) > r_i \deg G_i - g(F_i)\,.$$

So that by (b) and the right hand side inequality in (3.1) the information rate of $\mathcal{C}_i$ satisfies

$$\frac{k_i}{n_i} > \frac{r_i \deg G_i}{n_i} - \frac{g(F_i)}{n_i} \geq \frac{r_i \deg G_i}{n_i} - \ell \geq 1 - \delta - \epsilon - \ell$$

for $i \geq m = \max\{i_0, i_\epsilon\}$. Since ϵ can be arbitrarily small, we have

$$\limsup_{i\to\infty} \frac{k_i}{n_i} \geq 1 - \delta - \ell \qquad \text{and} \qquad \limsup_{i\to\infty} \frac{d_i}{n_i} \geq \delta,$$

so that the sequence of AG-codes $\{\mathcal{C}_i\}$ attains a (λ, δ)-bound as claimed. □

It is easy to see that in a concrete situation the crucial properties to have are conditions (b) and (c). In fact, once (a) and (b) are satisfied, condition (c) is not a problem unless we want the codes $\mathcal{C}_i$ to have some prescribed structure. More precisely, one can just consider $G_i = P_i$, where P_i is a rational place of F_i which is not in the support of D_i. However, this choice of G_i may not be adequate in certain cases like, for instance, the case when the invariance of G_i under some F_0-embedding of F_i is needed as it happens when a required structure of the constructed code is induced by the action of a Galois group.

Remark 3.2. Proposition 3.1 holds in the case of an asymptotically good tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ whose limit is bigger than 1. In fact, if N_i is the number of rational places of F_i then we can take $n_i = N_i - 1$, $G_i = Q_i$ (where Q_i is the rational place of F_i not considered among the chosen n_i rational places) and $s(i) = 1/n_i$. Then

$$\lim_{i\to\infty} \frac{n_i}{g(F_i)} = \lim_{i\to\infty} \frac{N_i - 1}{g(F_i)} > 1$$

so that there is an index i_0 such that (b) of Proposition 3.1 holds for all $i \geq i_0$. Clearly, items (a) and (c) also holds. Further, notice that if (b) holds using the sequence of function fields of a tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$, then

$$\lim_{i\to\infty} \frac{N_i}{g(F_i)} \geq \limsup_{i\to\infty} \frac{n_i}{g(F_i)} \geq \ell^{-1} > 1$$

so that the limit of the considered tower is bigger than 1.

Remark 3.3. The constant ℓ in (b) satisfies the estimate $\ell^{-1} \leq \sqrt{q} - 1$. To see this recall the upper bound of Drinfeld and Vladut for Ihara's function, namely $A(q) \leq \sqrt{q} - 1$. By definition of $A(q)$ we have that

$$A(q) \geq \frac{n_i}{g(F_i)} \geq \ell^{-1}\,, \tag{3.2}$$

and the claim follows. This bound also tell us that the construction of asymptotically good AG-codes over $\mathbb{F}_q$ provided by Lemma 3.1 can not be carried out for $q \leq 4$.

We now use Lemma 3.1 to give examples of asymptotically good AG-codes over $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$ and also over $\mathbb{F}_q$ for an arbitrary q large enough.

Example 3.4. For each $q > 2$ there is a family of AG-codes over $\mathbb{F}_{q^2}$ which is asymptotically good. To show this we just use the function fields in the recursive tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{q^2}$ of Garcia and Stichtenoth whose defining equation is

$$y^q + y = \frac{x^q}{x^{q-1}+1}\,.$$

It is known (see, for instance, [9, Example 5.4.1]) that $N(F_i) \geq q^{i-1}(q^2-q)+1$ and

$$g(F_i) = \begin{cases} (q^{\frac{i}{2}}-1)^2 & \text{for } i \text{ even,} \\ (q^{\frac{i-1}{2}}-1)(q^{\frac{i-2}{2}}-1) & \text{for } i \text{ odd.} \end{cases}$$

Thus, by taking $n_i = q^{i-1}(q^2-q)$, we have n_i+1 rational places $P_1^{(i)}, \ldots, P_{n_i}^{(i)}, Q_i$ in F_i and

$$\frac{n_i}{g(F_i)} \geq q-1\,,$$

for all $i \geq 1$. We readily see that condition (a) in Lemma 3.1 holds and the same happens with condition (b) with $\ell = (q-1)^{-1} = A(q)^{-1}$. Finally, by taking $G_i = Q_i$, we see that condition (c) also holds with $s(i) = 1/n_i$. In this way, by Lemma 3.1, the sequence $\{\mathcal{C}_i\}_{i\in\mathbb{N}}$ of AG-codes $\mathcal{C}_i = C(D_i, Q_i)$, with $D_i = P_1^{(i)} + \cdots + P_{n_i}^{(i)}$, is asymptotically good and attains the Tsfasman-Vladut-Zink bound over $\mathbb{F}_{q^2}$ for $q \geq 3$.

Serre's type lower bound for $A(q)$ give us a way to prove that the family of AG-codes over $\mathbb{F}_q$ is asymptotically good for any q large enough.

Example 3.5. It is well known ([9, Theorem 5.2.9]) that

$$A(q) \geq \tfrac{1}{96}\log_2 q\,,$$

for any prime power q. By definition of $A(q)$ there exists a sequence of function fields $\{F_i\}_{i=1}^{\infty}$ over $\mathbb{F}_q$ such that

$$\frac{N_i}{g(F_i)} \geq \tfrac{1}{96}\log_2 q > 1,$$

for $q > 2^{96}$, where $N_i = N(F_i)$. Take $n_i = N_i - 1$ and consider $\mathbb{F}_q$ with $q > 2^{96}$. Thus, condition (b) in Lemma 3.1 holds with $\ell = \frac{1}{96}\log_2 q$ and, since $g(F_i) \to \infty$ as $i \to \infty$, we must have that $N_i \to \infty$ as $i \to \infty$ so that condition (a) also holds. The divisor G_i is simply the remaining rational place of F_i after using the $N_i - 1$ rational places to define D_i. Clearly, condition (c) holds with $s(i) = 1/n_i$. Thus, by Lemma 3.1, there is a sequence of asymptotically good AG-codes over $\mathbb{F}_q$ attaining an (λ, δ)-bound for any $q > 2^{96}$ with $\lambda = 1 - \frac{1}{96}\log_2 q$ and $0 < \delta < \lambda$.

Example 3.6. By using a generalization of Zink's lower bound for $A(q^3)$ proved in [4], namely for any $q \geq 2$ we have

$$A(q^3) \geq \frac{2(q^2-1)}{q+2} > 1\,.$$

A similar argument as in Example 3.5 shows that for any q there is an asymptotically good AG-code over $\mathbb{F}_{q^3}$ attaining an (λ, δ)-bound with $\lambda = 1 - \frac{q+2}{2(q^2-1)}$ and $0 < \delta < \lambda$.

4. Asymptotically good 4-quasi transitive AG-codes over prime fields

From [12] and [2] we know that the class of transitive codes attains the Tsfasman-Vladut-Zink bound over $\mathbb{F}_{q^2}$ and the class of r-quasi transitive codes attains an (λ, δ)-bound over $\mathbb{F}_{q^3}$ with $\lambda = 1 - (q+2)/2r(q-1)$ and $0 < \delta < \lambda$. We prove now a general result for the case of 4-quasi transitive codes which will allow us to treat the case of prime fields.

First we quickly review some basic definitions used in the proof. The standard reference for all of this is [13]. Let F be a function field over K and let F' be a finite extension of F of degree n. Let Q be a place of F'. We will use the standard symbol $Q|P$ to say the place Q of F' lies over the place P of F, i.e. $P = Q \cap F$. In this case $e(Q|P)$ and $f(Q|P)$ denote, as usual, the ramification index and the relative (or inertia) degree of $Q|P$, respectively. Let P be a place of F. We say that P *splits completely* in F' if $e(Q|P) = f(Q|P) = 1$ for any place Q of F' lying over P. We say that P is *totally ramified* in F' if there is only one place Q of F' lying over P and $e(Q|P) = n$ (hence $f(Q|P) = 1$).

Theorem 4.1. *Let q be an odd prime power. Suppose there is a monic polynomial $h(t) \in \mathbb{F}_q[t]$ of degree 9 which splits into (different) linear factors over $\mathbb{F}_q$ and such that $h(\alpha)$ and $h(\beta)$ are nonzero squares in $\mathbb{F}_q$ for two different elements $\alpha, \beta \in \mathbb{F}_q$. Then there exists a sequence of asymptotically good 4-quasi transitive codes over $\mathbb{F}_q$ attaining an $(\frac{1}{8}, \delta)$-bound for $0 < \delta < \frac{1}{8}$.*

Proof. Let x be a transcendental element over $\mathbb{F}_q$. By [13, Proposition 6.3.1] we have that the equation

$$y^2 = h(x)$$

defines a cyclic Galois extension $F = \mathbb{F}_q(x, y)$ of degree 2 of $\mathbb{F}_q(x)$, where exactly 10 rational places of $\mathbb{F}_q(x)$ are (totally) ramified in F, 9 of them coming from the linear factors of $h(x)$ and another one defined by the pole P_∞ of x in $\mathbb{F}_q(x)$. Then, F is of genus 4 and $\mathbb{F}_q$ is its full constant field. Let P_α be the zero of $x - \alpha$ in $\mathbb{F}_q(x)$. Then the residual class

$$h(x)(P_\alpha) = h(\alpha) = \gamma^2\,,$$

for some $0 \neq \gamma \in \mathbb{F}_q$ by hypothesis. Thus the polynomial $t^2 - \gamma^2 \in \mathbb{F}_q[t]$ corresponds to the reduction mod P_α of the right hand side of the equation $y^2 = h(x)$.

By Kummer's theorem [13, Theorem 3.3.7] we have that P_α splits completely into two rational places Q_1 and Q_2 of F. The same argument shows that P_β also splits completely into two rational places Q_3 and Q_4 of F. Let Q_∞ be the only place of F lying above P_∞ and put

$$T = \{Q_\infty\} \qquad \text{and} \qquad S = \{Q_1, Q_2, Q_3, Q_4\}.$$

Since there are 10 ramified places of $\mathbb{F}_q(x)$ in F, the T-tamely ramified and S-decomposed Hilbert tower $\mathcal{H}_S^T$ of F is infinite (see [1, Corollary 11]). This means that there is a sequence $\{F_i\}_{i=0}^\infty$ of function fields over $\mathbb{F}_q$ such that $F_0 = F$,

$$\mathcal{H}_S^T = \bigcup_{i=1}^{\infty} F_i$$

and, for any $i \geq 1$, each place $Q \in S$ splits completely in F_i, the place Q_∞ is tamely ramified in F_i, F_i/F_{i-1} is an abelian extension with $[F_i : F] \to \infty$ as $i \to \infty$ and F_i/F_0 is unramified outside T.

Since S is a set of rational places of F which split completely in each F_i then each F_i has at least $4[F_i : F]$ rational places and $\mathbb{F}_q$ is the full constant field of F_i. Let g_i be the genus of

F_i. Since F_i/F is unramified outside T, the ramification is tame and Q_∞ is a ratioal place, Hurwitz's genus formula [13, Theorem 3.4.13] tell us that

$$\begin{aligned} 2g_i - 2 &= [F_i : F](2g-2) + \sum_{R \,|\, Q_\infty} (e(R|Q_\infty) - 1)\, \deg R \\ &\le 6[F_i : F] + \sum_{R \,|\, Q_\infty} e(R|Q_\infty)\, f(R|Q_\infty) = 7[F_i : F]\,, \end{aligned}$$

and therefore

$$g_i \le \tfrac{7}{2}[F_i : F] + 1\,.$$

Let F_i' be the Galois closure of F_i over F. From [13, Lemma 3.9.5] we have that the places of S of F split completely in F_i' so that F_i' is a function field over $\mathbb{F}_q$ whose full constant field is $\mathbb{F}_q$. In fact, the same lemma tell us that the extension F_i'/F is unramified outside T. Let Q' be a place of F_i' lying over Q_∞. Since the ramification is tame, from Abhyankar's Lemma [13, Theorem 3.9.1] we see that $e(Q'|Q_\infty) = e(Q|Q_\infty)$ where $Q = Q' \cap F_i$. Thus $e(Q'|Q) = 1$, which implies that the extension F_i'/F_i is unramified. If g_i' denotes the genus of F_i', from Hurwitz's genus formula we have

$$2g_i' - 2 = [F_i' : F_i](2g_i - 2) \le 7[F_i' : F],$$

so that

$$g_i' \le \tfrac{7}{2}[F_i' : F] + 1\,. \tag{4.1}$$

Let T_1 be the set of places of F_1 lying over Q_∞. Since the extension F_1/F is Galois (in fact, abelian) every place $P \in T_1$ is tamely ramified with ramification index $e = e(P|Q_\infty) \ge 2$ and relative degree $f = f(P|Q_\infty)$ so that $ref = [F_1 : F]$ where $r = |T_1|$. Then

$$\deg \sum_{P \in T_1} P = rf = \frac{[F_1 : F]}{e} \le \frac{[F_1 : F]}{2}\,.$$

Now suppose that

$$\deg \sum_{P \in T_{i-1}} P \le \frac{[F_{i-1} : F]}{2^{i-1}}\,,$$

where T_{i-1} is the set of places of F_{i-1} lying over Q_∞. Let $P \in T_{i-1}$ and let $R_1, \dots, R_{r_P}$ be all the places of F_i lying over P. Since F_i/F_{i-1} is a Galois extension, every place R_j over P is tamely ramified with the same ramification index e_P and relative degree f_P. Thus $r_P \cdot e_P \cdot f_P = [F_i : F_{i-1}]$ and then

$$r_P\, f_P = \frac{[F_i : F_{i-1}]}{e_P} \le \frac{[F_i : F_{i-1}]}{2}\,.$$

Hence, by inductive hypothesis, we have

$$\begin{aligned} \deg \sum_{R \in T_i} R &= \sum_{P \in T_{i-1}} r_P f_P \deg P \le \tfrac{1}{2}[F_i : F_{i-1}] \sum_{P \in T_{i-1}} \deg P \\ &\le \frac{[F_i : F_{i-1}]}{2} \frac{[F_{i-1} : F]}{2^{i-1}} = \frac{[F_i : F]}{2^i}\,, \end{aligned}$$

where T_i is the set of places of F_i lying over Q_∞. We have proved that if T_i is the set of places of F_i lying over Q_∞ then

$$\deg \sum_{P \in T_i} P \le \frac{[F_i : F]}{2^i}, \tag{4.2}$$

for all $i \in \mathbb{N}$.

Now we define the divisor

$$G_i = R_1 + \cdots + R_{k_i}$$

of F_i' where $R_1, \ldots, R_{k_i}$ are all the places of F_i' lying above Q_∞. Note that $\operatorname{Sup} G_i \cap F_i = T_i$ and if we denote by $R_1^P, \ldots, R_{n_P}^P$ all the places in $\operatorname{Sup} G_i$ lying over a place $P \in T_i$ we have that

$$\begin{aligned}\deg G_i &= \sum_{j=1}^{k_i} \deg R_j = \sum_{P \in T_i} \sum_{t=1}^{n_P} \deg R_t^P \\ &= \sum_{P \in T_i} \sum_{t=1}^{n_P} f(R_t^P|P)\, f(P|Q_\infty) = \sum_{P \in T_i} f(P|Q_\infty) \sum_{t=1}^{n_P} f(R_t^P|P) \\ &\leq \sum_{P \in T_i} f(P|Q_\infty)[F_i' : F_i] = [F_i' : F_i] \deg \sum_{P \in T_i} P \leq \frac{[F_i' : F]}{2^i}\,,\end{aligned}$$

by (4.2).

On the other hand, since the 4 rational places of S split completely in F_i', we have $n_i = 4[F_i' : F]$ rational places $S_1, \ldots, S_{n_i}$ of F_i' which are the ones lying over the places of S. Thus by (4.1) we have

$$\frac{g_i'}{n_i} \leq \frac{7}{8} + \frac{1}{n_i} \sim \frac{7}{8}\,,$$

for n_i big enough.

In this way we see that, condition (a) of Lemma 3.1 holds and condition (b) also holds with $\ell \sim 7/8 < 1$. By taking $D_i = S_1 + \cdots + S_{n_i}$ and $G_i = R_1 + \cdots + R_{k_i}$ we have that (c) holds with $s(i) = 2^{-(i+2)}$ so that the sequence $\{\mathcal{C}_i\}_{i=1}^\infty$ of AG-codes $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$ is asymptotically good over $\mathbb{F}_q$ attaining a $(\frac{1}{8}, \delta)$-bound with $0 < \delta < 1/8$. Finally notice that both divisors D_i and G_i are invariant under $\operatorname{Gal}(F_i'/F)$ so that by the definition of D_i and the action of $\operatorname{Gal}(F_i'/F)$ on the places in the support of D_i, we see at once that $C_{\mathcal{L}}(D_i, r_i G_i)$ is a 4-quasi transitive AG-code over $\mathbb{F}_q$. □

Corollary 4.2. *Let $q = p^r$ be an odd prime power. Suppose there are 4 distinct elements α_1, α_2, α_3, $\alpha_4 \in \mathbb{F}_q$ such that $\alpha_i^{-1} \notin \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for $1 \leq i \leq 4$ and consider the polynomial*

$$h(t) = (t+1) \prod_{i=1}^{4} (t - \alpha_i)(t - \alpha_i^{-1}) \in \mathbb{F}_q[t]\,. \tag{4.3}$$

Suppose also that there exists an element $\alpha \in \mathbb{F}_q^*$ such that $h(\alpha)$ is a nonzero square in $\mathbb{F}_q$. Then there exists a sequence of 4-quasi transitive codes over $\mathbb{F}_q$ which is asymptotically good attaining a $(\frac{1}{8}, \delta)$-bound with $0 < \delta < \frac{1}{8}$.

Proof. The conclusion follows directly from Theorem 4.1 by noticing that $h(0) = 1$, which is a nonzero square in $\mathbb{F}_q$. □

Example 4.3. It is easy to check that for $p = 11$ there is no separable polynomial of degree 9 satisfying the conditions required in Theorem 4.1. Let $p = 13$, 17, 19 and 23. It is straightforward to check that the elements $\alpha_1 = 2$, $\alpha_2 = 3$, $\alpha_3 = 4$ and $\alpha_4 = 5$ of $\mathbb{F}_p$

with $p = 13, 17$ or 23 satisfy the conditions of Corollary 4.2 and

$$h(t) = (t+1)(t-2)(t-7)(t-3)(t-9)(t-4)(t-10)(t-5)(t-8) \in \mathbb{F}_{13}[t],$$
$$h(t) = (t+1)(t-2)(t-9)(t-3)(t-6)(t-4)(t-13)(t-5)(t-9) \in \mathbb{F}_{17}[t],$$
$$h(t) = (t+1)(t-2)(t-12)(t-3)(t-8)(t-4)(t-6)(t-5)(t-14) \in \mathbb{F}_{23}[t].$$

Thus, by taking $\alpha = 11 \in \mathbb{F}_{13}$ we have that $h(11) = 3 = 4^2$ in $\mathbb{F}_{13}$. Similarly, by choosing $\alpha = 1 \in \mathbb{F}_{17}$ and $\alpha = 7 \in \mathbb{F}_{23}$ we get $h(1) = 13 = 8^2$ in $\mathbb{F}_{17}$ and $h(7) = 3 = 7^2$ in $\mathbb{F}_{23}$, respectively.

Finally, the elements $\alpha_1 = 2$, $\alpha_2 = 3$, $\alpha_3 = 4$ and $\alpha_4 = 6$ of $\mathbb{F}_{19}$ also satisfy the conditions of Corollary 4.2 and

$$h(t) = (t+1)(t-2)(t-10)(t-3)(t-13)(t-4)(t-5)(t-6)(t-16)\,,$$

so that by taking $\alpha = 12 \in \mathbb{F}_{19}$ we have that $h(12) = 4 = 2^2$ in $\mathbb{F}_{19}$.

Therefore, from Corollary 4.2, we see that there are sequences of 4-quasi transitive codes over $\mathbb{F}_p$ for $p = 13, 17, 19$ and 23 which are asymptotically good attaining a $(\frac{1}{8}, \delta)$-bound with $0 < \delta < \frac{1}{8}$.

Example 4.4. We now consider the case of an arbitrary prime $p \geq 29$. By Fermat's theorem the inverse of a in $\mathbb{F}_p$ is a^{p-2} and, hence, (4.3) takes the form

$$h(t) = (t+1)\prod_{k=2}^{5}(t-k)(t-k^{p-2}).$$

in $\mathbb{F}_p[t]$. We want to find an element $a \in \mathbb{F}_p^*$ such that $h(a)$ is a nonzero square in $\mathbb{F}_p$. It suffices to check that $\left(\frac{h(a)}{p}\right) = 1$, where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo p. Since the Legendre symbol is multiplicative, we have

$$\left(\tfrac{h(t)}{p}\right) = \left(\tfrac{t+1}{p}\right)\prod_{k=2}^{5}\left(\tfrac{t-k}{p}\right)\left(\tfrac{t-k^{p-2}}{p}\right).$$

Evaluating $h(t)$ at $t = p - j$ for $2 \leq j \leq \lfloor \frac{p-1}{5} \rfloor$ we have that $h(p-j) \neq 0$ and

$$h(p-j) = (p-(j-1))\prod_{k=2}^{5}(p-(j+k))(p-(j+k^{p-2})).$$

Now, computing the Legendre symbol of $h(p-j)$, we get

$$\left(\tfrac{h(p-j)}{p}\right) = \left(\tfrac{1-j}{p}\right)\prod_{k=2}^{5}\left(\tfrac{j+k}{p}\right)\left(\tfrac{k}{p}\right)^2\left(\tfrac{j+k^{p-2}}{p}\right) = \left(\tfrac{1-j}{p}\right)\prod_{k=2}^{5}\left(\tfrac{j+k}{p}\right)\left(\tfrac{k}{p}\right)\left(\tfrac{kj+1}{p}\right)$$

where we have used that $(\frac{k}{p})^2 = 1$. For instance, for $p \geq 37$ we can take the $j = 2, \ldots, 7$ and in this case we have

$$\left(\tfrac{h(p-2)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{5}{p}\right)\left(\tfrac{11}{p}\right), \qquad \left(\tfrac{h(p-3)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right)\left(\tfrac{5}{p}\right)\left(\tfrac{13}{p}\right),$$
$$\left(\tfrac{h(p-4)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right)\left(\tfrac{5}{p}\right)\left(\tfrac{13}{p}\right)\left(\tfrac{17}{p}\right), \qquad \left(\tfrac{h(p-5)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{11}{p}\right)\left(\tfrac{13}{p}\right),$$
$$\left(\tfrac{h(p-6)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right)\left(\tfrac{3}{p}\right)\left(\tfrac{5}{p}\right)\left(\tfrac{11}{p}\right)\left(\tfrac{13}{p}\right)\left(\tfrac{19}{p}\right)\left(\tfrac{31}{p}\right), \quad \left(\tfrac{h(p-7)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right)\left(\tfrac{29}{p}\right).$$

This reduces the search of a nonzero element $\alpha \in \mathbb{F}_p$ such that $h(\alpha)$ is a nonzero square in $\mathbb{F}_p$ to the computation of Legendre symbols for a given prime $p \geq 37$.

Corollary 4.5. *There are asymptotically good 4-quasi transitive AG-codes over $\mathbb{F}_p$ for infinite primes p. For instance, this holds for primes of the form $p = 220k + 1$ or $p = 232k + 1$, $k \in \mathbb{N}$.*

Proof. We consider the polynomial $h(t) = (t+1)\prod_{k=2}^{5}(t-k)(t-k^{p-2})$ as in Example 4.4. By Corollary 4.2, it suffices to find infinitely many primes p, such that $\left(\frac{h(p-j)}{p}\right) = 1$, for a given j. Consider first $j = 2$. We look for prime numbers p such that

$$\left(\tfrac{h(p-2)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{5}{p}\right)\left(\tfrac{11}{p}\right) = 1.$$

Since $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \bmod 4$ and $\left(\frac{5}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 5$, it is clear that if p is of the form $p = 20k + 1$ then $\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1$. In this way, for prime numbers of the form $p = (20 \cdot 11)k + 1$, $k \in \mathbb{N}$, we have that $\left(\frac{h(p-2)}{p}\right) = 1$.

Now consider $j = 7$. Now we look for prime numbers p such that

$$\left(\tfrac{h(p-7)}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right)\left(\tfrac{29}{p}\right) = 1.$$

Since $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 8$ we have that if p is of the form $p = 8k+1$ then $\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ and hence $\left(\frac{h(p-7)}{p}\right) = 1$ for primes of the form $p = (8 \cdot 29)k + 1$, $k \in \mathbb{N}$.

By Dirichlet's theorem on arithmetic progressions, there are infinitely many prime numbers of the form $p = 220k+1$ and $p = 232k+1$ with $k \in \mathbb{N}$, and thus the result follows. □

Remark 4.6. As we have already seen, there are families of asymptotically good 4-quasi transitive AG-codes over prime fields $\mathbb{F}_p$ for infinitely many primes p. It is computationally easy to check that Corollary 4.2 holds true, in fact, for all primes $19 < p < 10^6$ with $\alpha_1 = 2$, $\alpha_2 = 3$, $\alpha_3 = 4$ and $\alpha_4 = 5$ as in Example 4.4. These numerical experiments suggest that Corollary 4.2 holds true for any prime $p \geq 13$ using the polynomial given in Example 4.4, except for $p = 19$.

5. Some remarks on the asymptotic behavior of cyclic AG-codes

Let F be a function field over $\mathbb{F}_q$. Recall that an AG-code $C_{\mathcal{L}}(D, G)$ with $D = P_1 + \cdots + P_n$ is cyclic if for any codeword

$$(u(P_1), \ldots u(P_n)) \in C_{\mathcal{L}}(D, G),$$

where $u \in \mathcal{L}(G)$, we have that

$$(u(P_n), u(P_1), \ldots u(P_{n-1})) \in C_{\mathcal{L}}(D, G).$$

Clearly this happens if and only if for each $(u(P_1), , \ldots u(P_{n-1}), u(P_n)) \in C_{\mathcal{L}}(D, G)$ there exists $z \in \mathcal{L}(G)$ such that $z(P_i) = u(P_{i-1 \bmod n})$ for $i = 1, \ldots, n$, i.e.

$$\begin{array}{rcl} z(P_1) & = & u(P_n)\,, \\ z(P_2) & = & u(P_1)\,, \\ & \vdots & \\ z(P_n) & = & u(P_{n-1})\,. \end{array} \tag{5.1}$$

The existence of such an element $z \in \mathcal{L}(G)$ is a crucial question to answer in the theory of cyclic AG-codes. So far, a positive answer can be given when the places in the support of D belong to a finite cyclic extension F/E, for some function field $\mathbb{F}_q(x) \subset E \subset F$, and they are lying over a unique place of E. To see this, let us consider the group $\mathrm{Aut}(F/\mathbb{F}_q(x))$ of

all $\mathbb{F}_q(x)$-automorphisms of F, where $x \in F$ is transcendental over $\mathbb{F}_q$. Suppose we can find an element $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q(x))$ such that

$$\sigma(G) = G \quad \text{and} \quad \sigma(P_1) = P_n,\ \sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}.$$

Then, we clearly have that $\sigma(D) = D$ and the element $z = \sigma^{-1}(u)$ of F does the job. In fact, $z \in \mathcal{L}(G)$, because $\sigma(Q) \in \mathrm{Sup}\, G$ for any $Q \in \mathrm{Sup}\, G$, and so

$$\nu_Q(z) = \nu_{\sigma(Q)}(z) \geq -\nu_{\sigma(Q)}(G) = -\nu_Q(\sigma^{-1}G) = -\nu_Q(G),$$

which means that $(z) \geq -G$ and further

$$z(P_i) = \big(\sigma^{-1}(u)\big)(P_i) = u(\sigma(P_i)) = u(P_{i-1 \bmod n}),$$

for $i = 1, \ldots, n$, so that (5.1) holds.

We will show now that the situation above described can happen only in the presence of cyclic extensions.

Proposition 5.1. *Let F be a function field over $\mathbb{F}_q$ and let $P_1, \ldots, P_n$ be n different places of F. Suppose there exists $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q(x))$ such that $\sigma(P_1) = P_n$, $\sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}$. Then there exist an intermediate field $\mathbb{F}_q(x) \subset E \subset F$ and a place P of E such that F/E is a cyclic extension of degree m divisible by n, and P decomposes exactly in F into the places $P_1, \ldots, P_n$ with $e(P_i|P)f(P_i|P) = \frac{m}{n}$ for $i = 1, \ldots, n$. Conversely, let F/E be a cyclic extension of function fields over $\mathbb{F}_q$ of degree m. Let P be a place of E and let $P_1, \ldots, P_n$ be all the places of F lying over P. Then, m is divisible by n and we have that $\sigma(P_1) = P_n$, $\sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}$ for any generator σ of $\mathrm{Gal}(F/E)$.*

Proof. Let G be the subgroup of $\mathrm{Aut}(F/\mathbb{F}_q(x))$ generated by σ and let $E = F^G$, the fixed field of G. Thus, F/E is a cyclic extension of degree m with Galois group

$$\mathrm{Gal}(F/E) = G = \langle \sigma \rangle,$$

where m is the order of σ in $\mathrm{Aut}(F)$. Clearly $\mathbb{F}_q(x) \subset E$.

Let $P = P_1 \cap E$. Then P is a place of E and, since $\sigma(P_i) = P_{i-1 \bmod n}$ for $i = 1, \ldots, n$ we also have that $P = P_i \cap E$ for $i = 1, \ldots, n$. These are, in fact, all the places of F lying above P, because G acts transitively on the set of places of F lying above P.

On the other hand we have the fundamental relation

$$\sum_{i=1}^{n} e(P_i|P)f(P_i|P) = [F : E] = m.$$

Since F/E is Galois, we have that $e(P_i|P) = e$ and $f(P_i|P) = f$, for $i = 1, \ldots, n$. Thus $nef = m$ and we are done with the first part.

Suppose now that F/E is a cyclic extension of degree m. By the fundamental relation in Galois extensions, n divides m. Let σ be a generator of $G = \mathrm{Gal}(F/K)$. If $\sigma^i(P_1) = \sigma^j(P_1)$ for some $1 \leq i < j \leq n$ then, for $k = j - i > 0$,

$$\sigma^k \in D(P_1|P) = \{\sigma \in G : \sigma(P_1) = P_1\},$$

the decomposition group of P_1 over P. Since $D(P_1|P)$ is of order ef, where $e = e(P_i|P)$ and $f = f(P_i|P)$ for $i = 1, \ldots, n$, we have that $\sigma^{kef} = 1$. But $k < n$ and so $kef < nef = m$ contradicting that m is the order of σ. Therefore $\{\sigma^i(P_1)\}_{i=1}^n$ are all distinct places of F so that

$$\{\sigma(P_1), \sigma^2(P_1), \ldots, \sigma^n(P_1)\} = \{P_1, P_2, \ldots, P_n\}.$$

This implies that $\sigma(P_1) = P_n$, $\sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}$, after a possible renumbering of the indices of the places of F lying above P. □

Few things are known, so far, with regard to the asymptotic behavior of the class of cyclic codes. Perhaps the most interesting result in this direction is the one due to Castagnoli who proved in [5] that the class of cyclic codes whose block lengths have prime factors belonging to a fixed finite set of prime numbers is asymptotically bad. This result implies that the construction of cyclic AG-codes in the standard way, i.e. by using an asymptotically good recursive tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ and a rational place of F_0 which splits completely in the tower $\mathcal{F}$, would lead to a sequence of codes asymptotically bad because the block lengths of these codes is $n^i = [F_i : F_0]$ for $i \geq 1$, where n is the degree in both variables of the bivariate polynomial defining the tower $\mathcal{F}$.

Even more can be said, as we show now in the next result. We shall need to introduce first the *ramification locus*, $\mathrm{Ram}(\mathcal{F})$, of a tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$, which is simply the set of all places of F_0 which are ramified in the tower, i.e.

$$\mathrm{Ram}(\mathcal{F}) = \{P \in F_0 \,:\, e(Q|P) > 1,\, Q \in \mathbb{P}(F_i),\, i \in \mathbb{N}\}.$$

This set plays a decisive role in the asymptotic behavior of towers (see, for example, Chapter 7 of [13]).

Theorem 5.2. *Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be an asymptotically good tower (not necessarily recursive) of function fields over $\mathbb{F}_q$ where $F_0 = \mathbb{F}_q(x)$ is a rational function field. For each $i \in \mathbb{N}$, let n_i be a positive integer and let $P_1, \ldots, P_{n_i}$ be different rational places of F_i. Suppose that for each $i \in \mathbb{N}$ there is an element $\sigma_i \in \mathrm{Aut}(F_i/F_0)$ such that*

$$\sigma(P_1) = P_{n_i},\ \sigma(P_2) = P_1,\ \ldots,\ \sigma(P_{n_i}) = P_{n_i - 1}.$$

Then $n_i < [F_i : F_0]$ and there exists a place $P \in \mathrm{Ram}(\mathcal{F})$ such that the places of F_i lying over P are exactly $P_1, \ldots, P_{n_i}$.

Proof. Suppose that each $n_i \geq [F_i : F_0]$. From Proposition 5.1 we see that there is a subfield K_i of F_i such that F_i/K_i is cyclic of degree m_i with n_i dividing m_i. Since K_i is the fixed field of σ_i, we have that $F_0 \subset K_i$ so that $m_i \leq [F_i : F_0]$. Then $n_i = m_i = [F_i : F_0]$ and this implies that $K_i = F_0$ so that F_i/F_0 is a cyclic extension for each $i \geq 0$. This leads to a contradiction because it was proved in [6] that abelian towers are asymptotically bad. Therefore, $n_i < [F_i : F_0]$ and the above argument together with Proposition 5.1 show that $F_0 \subsetneq K_i$ and that there is a rational place Q_i of K_i such that P_j lies above Q_i for $j = 1, \ldots, n_i$. If $R_i = F_0 \cap Q_i$, then R_i is a rational place of F_0 which is totally ramified in K_i, because the relative degree $f(Q_i|R_i) = 1$. Therefore $R_i \in \mathrm{Ram}(\mathcal{F})$ and clearly all the places of F_i lying over R_i are exactly $P_1, \ldots, P_{n_i}$. □

Final remarks. The above result shows how different the situation is when dealing with the asymptotic behavior of transitive (or quasi transitive) AG-codes and cyclic AG-codes, which are particular cases of transitive AG-codes. In the case of transitive or quasi transitive AG-codes, in each step of the tower, we have that the divisor D in the AG-code $C_{\mathcal{L}}(D, G)$ is defined using all the rational places lying over a totally split rational place of a rational function field $\mathbb{F}_q(x)$. This situation is what makes possible to prove the good asymptotic behavior of transitive or quasi transitive AG-codes.

On the other hand, for the case of cyclic AG-codes, Theorem 5.2 shows that not only this is not possible, but also that the divisor D has to be defined with all the rational places lying over a place in the ramification locus of the tower. From this, we arrive to a bit surprising conclusion. Namely, that towers with only totally ramified places in the tower, which are nice candidates for good asymptotic behavior, have to be discarded for the construction of potentially good sequences of cyclic AG-codes, if we want to use all

the techniques and results that were successful in the transitive case. All of this, together with Castagnoli's result, provide some good reasons to think that towers of function fields may not be adequate to address the problem of the asymptotic behavior of cyclic codes, as long as the sequence of cyclic AG-codes is constructed using automorphisms of the function fields in the tower.

Thus it is clear that the design of new methods to produce cyclic AG-codes is an interesting and challenging problem with potential consequences in the study of the asymptotic behavior of cyclic codes. In particular, it would be interesting to see if it is possible to construct cyclic AG-codes without using automorphisms of the involved function fields. This would be a matter of research that we plan to deal with in the near future.

References

[1] B. Angles and C. Maire. A note on tamely ramified towers of global function fields. *Finite Fields Appl.*, 8(2):207–215, 2002.

[2] A. Bassa. Towers of function fields over cubic fields. phd thesis, duisburg-essen university. 2006.

[3] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth. An improvement of the gilbert-varshamov bound over nonprime fields. *IEEE Trans. Inform. Theory*, 60(7):3859–3861, 2014.

[4] J. Bezerra, A. Garcia, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *J. Reine Angew. Math.*, 589:159–199, 2005.

[5] G. Castagnoli. On the asymptotic badness of cyclic codes with block-lengths composed from a fixed set of prime factors. In *Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988)*, volume 357 of *Lecture Notes in Comput. Sci.*, pages 164–168. Springer, Berlin, 1989.

[6] G. Frey, M. Perret, and H. Stichtenoth. On the different of abelian extensions of global fields. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 26–32. Springer, Berlin, 1992.

[7] E. Martínez-Moro, C. Munuera, and D. Ruano, editors. *Advances in algebraic geometry codes*, volume 5 of *Series on Coding Theory and Cryptology*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008.

[8] C. Moreno. *Algebraic curves over finite fields*, volume 97 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1991.

[9] H. Niederreiter and C. Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2001.

[10] J.P. Serre. Rational points on curves over finite fields. Unpublished lecture notes by F. Q. Gouvea, Harvard University, 1985.

[11] S. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum Publishers, New York, 1999.

[12] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound. *IEEE Trans. Inform. Theory*, 52(5):2218–2224, 2006.

[13] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[14] M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[15] S. Vlàdut and V. Drinfel'd. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.

María Chara – Instituto de Matemática Aplicada del Litoral - UNL - CONICET, (3000) Santa Fe, Argentina. *E-mail: mchara@santafe-conicet.gov.ar*

Ricardo Podestá – CIEM-CONICET, FaMAF, Universidad Nacional de Córdoba, (5000) Córdoba, Argentina. *E-mail: podesta@famaf.unc.edu.ar*

Ricardo Toledano – FIQ-IMAL-UNL-CONICET, Departamento de Matemática, Facultad de Ingeniería Química, Stgo. del Estero 2829, (3000) Santa Fe, Argentina. *E-mail: ridatole@gmail.com*